Notas de la versión de PGP(R) Desktop versión 10.0 para Windows

Gracias por utilizar este producto de PGP Corporation. Estas Notas de la versión contienen información importante respecto a esta versión de PGP Desktop para Windows. PGP Corporation recomienda leer el documento completo.

PGP Corporation agradecerá sus comentarios y sugerencias. Utilice la información proporcionada en Cómo obtener ayuda para comunicarse con nosotros.

Producto: PGP Desktop para Windows

Versión: 10.0.2

Advertencia: la exportación de este software puede ser restringida por el gobierno de los Estados Unidos.

Nota: para visualizar la versión más reciente de este documento, visite el portal de soporte técnico para PGP y consulte el artículo de la base de conocimiento *Guías del usuario de PGP, Guías del administrador, Guías del administrador y Notas de la versión*.

Qué encontrará en este archivo

- Acerca de PGP Desktop
- Cambios en esta versión
- Requisitos del sistema
- Instrucciones de instalación
- Licencia
- Información adicional
- Cómo obtener ayuda
- Derechos de autor y marcas comerciales

Acerca de PGP Desktop para Windows

PGP Desktop es una herramienta de seguridad que utiliza criptografía para proteger sus datos contra accesos no autorizados.

Cambios en esta versión

Esta sección enumera los cambios y las nuevas funciones de esta versión de PGP Desktop.

Novedades en PGP Desktop para Windows versión 10.0

Aprovechando la tecnología de probada eficacia de PGP Corporation, PGP Desktop 10.0 para Windows incluye numerosas mejoras y las siguientes nuevas funciones.

PGP Desktop Versión 10.0.2

- No se incluyen características nuevas en esta versión.

PGP Desktop Versión 10.0.1

- Esta versión de PGP Desktop incluye la resolución de problemas menores. No se incluyen características nuevas en esta versión.

PGP Desktop Versión 10.0.0

General

- **Otros sistemas operativos compatibles**. PGP Desktop para Windows puede instalarse en Windows 7.
- **Nuevas versiones localizadas**. PGP Desktop se ha localizado y ahora se puede instalar en francés (Francia)

y español (Latinoamérica).

- **Compatibilidad con nuevas tarjetas inteligentes**. Tanto para el arranque previo como para el arranque posterior en PGP Desktop para Windows:
  - Tarjeta inteligente Axalto Cyberflex Access 32K V2
  - Tarjetas de verificación de identidad personal Giesecke and Devrient Sm@rtCafe Expert 3.2
  - Tarjetas de verificación de identidad personal Oberthur ID-One Cosmo V5.2D
  - Token USB SafeNet iKey 2032
  - Tarjetas T-Systems Telesec NetKey 3.0 y TCOS 3.0 IEI
- **Nuevo diseño de interfaz**. La ventana principal de la aplicación de usuario de PGP Desktop para Windows cuenta con un nuevo diseño.
- **Conectividad de PGP Universal Server**. Mayor resistencia de PGP Desktop cuando la conectividad con PGP Universal Server depende de una conexión VPN o es intermitente.

Llaves PGP

- **Llaves Server Key Mode (SKM) (Modo de llave servidor [SKM]) mejoradas**. Las llaves SKM ahora incluyen toda la llave en su anillo de llaves. Además, ahora se pueden utilizar para funciones de encriptación, por ejemplo, para encriptar y desencriptar discos y archivos, así como para desencriptar mensajes de correo electrónico de MAPI cuando está fuera de línea.
- **Ubicación del anillo de llaves**. En PGP Desktop para Windows, puede utilizar las variables de entorno para especificar la ubicación de sus anillos de llaves.
- **Indicadores de uso de llave**. Ahora, cada subllave puede tener sus propiedades de uso de llave, de modo que una subllave se pueda usar sólo para PGP WDE y otra se pueda usar para el resto de las funciones de PGP Desktop. Establezca el uso de llave cuando desee utilizar una llave sólo para encriptar discos y no desee recibir correo electrónico encriptado con esa llave.
- **Búsquedas de llaves de Universal Server Protocol (USP)**. El Protocolo de servicios de PGP Universal (USP) es un protocolo SOAP que funciona con puertos HTTP/HTTPS estándar. Ahora, este es el mecanismo predeterminado de búsqueda de llaves. Si se encuentra en un entorno gestionado por PGP Universal Server, todas las solicitudes de búsqueda de llaves y el resto de las comunicaciones que haya entre PGP Universal Server y PGP Desktop utilizan PGP USP.

Mensajería de PGP

- **PGP Viewer**. Utilice PGP Viewer para desencriptar y ver mensajes de correo electrónico de IMAP/POP/SMTP heredados.
- **Lotus Notes**. Ahora, PGP Desktop le permite encriptar mensajes de correo con la encriptación nativa de Lotus Notes si PGP Desktop está configurado para hacerlo y el destinatario es usuario interno de Notes.
- **Lotus Notes**. Ahora, PGP Desktop permite encriptar mensajes de correo electrónico de formato RTF con Lotus Notes utilizando formatos de PGP/MIME, S/MIME o PGP particionado.
- **Lotus Notes**. Ahora, las anotaciones de PGP en los mensajes respetan la configuración regional en la marca de tiempo y fecha.
- **Botones agregados de Microsoft Outlook**. Los botones le permiten agregar manualmente la encriptación o su firma digital a los correos electrónicos de Outlook. Esta nueva función cumple con las leyes de firma digital que exigen que se demuestre la intención de firmar.
- **Mejoras en la política fuera de línea**. Ahora, en los entornos gestionados, la política de correo se aplica, incluso, si se está fuera de línea y no se está conectado a PGP Universal Server, o si el mismo servidor está fuera de línea.

PGP Portable

- Antes estaba disponible como opción independiente, ahora PGP Portable está incluido en PGP Desktop. Se pueden crear discos de PGP Portable en los sistemas de Windows. Esta funcionalidad requiere otra licencia.

PGP Whole Disk Encryption

- **Compatibilidad adicional con tarjetas inteligentes**. Se han agregado nuevas tarjetas para la autenticación del arranque previo en PGP Whole Disk Encryption para Windows: Axalto Cyberflex Access 32K V2, , el token

USB Marx CrypToken, el token USB SafeNet iKey 2032 y la tarjeta inteligente T-Systems T-Telesec NetKey.

- **Compatibilidad con tarjetas de verificación de identidad personal (PIV)**. Se ha agregado compatibilidad en PGP Whole Disk Encryption para Windows, para los usuarios que tienen tarjetas de verificación de identidad personal Giesecke and Devrient Sm@rtCafe Expert 3.2 y Oberthur ID-One Cosmo V5.2D.
- **Compatibilidad con más teclados (Windows)**. Ahora se puede utilizar un total de 50 teclados en idiomas internacionales para iniciar sesión en PGP BootGuard. Para obtener una lista de todos los teclados compatibles, consulte la Guía del usuario de PGP Desktop para Windows o la ayuda en pantalla.
- **Compatibilidad para encriptación de discos completos en Linux**. PGP WDE para Linux permite encriptar discos completos con autenticación del arranque previo en Ubuntu y Red Hat. Para obtener más información, consulte la Guía de PGP Whole Disk Encryption para las líneas de comando de Linux.
- **Recuperación automática local**. Ahora, PGP Desktop para Windows le brinda una opción para tener acceso a su unidad encriptada desde la pantalla de PGP BootGuard si olvidó su contraseña. Cuando esta opción esté configurada, no debe comunicarse con el administrador para solicitar asistencia.
- **Mejoras para usuarios múltiples**. En los entornos donde usuarios múltiples pueden tener acceso a un grupo de computadoras, el administrador de PGP Universal Server puede establecer una contraseña de administrador para PGP WDE. Cuando ingrese esta contraseña en la pantalla de PGP BootGuard en PGP Desktop para un sistema de Windows, se le solicita que ingrese su contraseña de Windows y el disco se desencripta.
- **Mejoras para la encriptación forzada**. Cuando el administrador de PGP Universal Server modifique la política para exigir que todos los discos estén encriptados, la próxima vez que la política se descargue en su sistema aparece el asistente de PGP WDE para que pueda comenzar a encriptar el disco.
- **Compatibilidad con más tokens en PGP BootGuard**. Ahora, el token USB Marx CrypToken se puede utilizar en PGP BootGuard de PGP Desktop para Windows.
- **Compatibilidad con caracteres ASCII extendidos**. Ahora se pueden utilizar caracteres ASCII extendidos al crear usuarios de PGP WDE.
- **Caracteres kanji**. Ahora, los caracteres kanji aparecen correctamente en la pantalla de PGP BootGuard.
- **Sistemas operativos Windows Server**. PGP WDE ahora se puede instalar en los sistemas operativos Windows Server (Windows Server 2003 y Windows Server 2008). Para obtener más información acerca de los requisitos del sistema y de las mejores prácticas para el uso de PGP WDE en Windows Server, consulte el Artículo 1737 de la Base de conocimientos de PGP.

Problemas resueltos

Para obtener una lista de los problemas que se han resuelto en esta versión, visite el Portal de soporte técnico para PGP y consulte el Artículo 1014 de la Base de conocimientos.

Requisitos del sistema

- Microsoft Windows 2000 (Service Pack 4),

  > **Nota:** los sistemas operativos mencionados anteriormente serán compatibles únicamente cuando se hayan aplicado todas las reparaciones en caliente y los parches de seguridad más recientes de Microsoft.

  PGP Whole Disk Encryption (WDE) es compatible con todas las versiones del cliente mencionadas anteriormente y con las siguientes versiones de Windows Server:

  - Windows Server 2003 SP 2 (ediciones de 32 y 64 bits)
  - Windows Server 2008 SP 1 y 2 (ediciones de 32 y 64 bits)
  - Windows Server 2008 R2 (ediciones de 32 y 64 bits)

    Para obtener más información acerca de los requisitos del sistema y de las mejores prácticas para el uso de PGP WDE en Windows Server, consulte el Artículo 1737 de la Base de conocimientos de PGP.

- 512 MB de RAM
- 64 MB de espacio en disco

Software de cliente de correo electrónico compatible

En muchos casos, PGP Desktop para Windows funcionará con clientes de correo electrónico basados en estándares de Internet diferentes a los enumerados aquí. Sin embargo, PGP Corporation no admite el uso de otros clientes.

PGP Desktop para Windows se ha probado con los siguientes clientes de correo electrónico:

- Microsoft Outlook 2007 SP1 (Outlook 12)
- Microsoft Outlook 2003 SP3
- Microsoft Outlook XP SP3
- Microsoft Windows Mail 6.0.600.16386
- Microsoft Outlook Express 6 SP1
- Windows Live Mail versión 2009
- Mozilla Thunderbird 2.0
- Lotus Notes 6.5.6, 7.0.3, 8.02, 8.5
- Novell GroupWise 6.5.1

Estado de compatibilidad de PGP Corporation con Microsoft Exchange Server 2007

PGP Corporation se enorgullece de anunciar su compatibilidad con el nuevo Exchange Server 2007 de Microsoft. PGP Desktop 9.6 presentó el soporte técnico para Microsoft Exchange Server y Microsoft Office 2007. Cuando se utiliza con mensajes PGP/MIME (RFC 3156) estándar de Internet, se preserva la fidelidad del mensaje completo en todos los mensajes seguros.

Con Exchange Server 2007, Microsoft ha introducido un cambio en funcionalidad que convierte todos los mensajes a su formato MAPI interno inmediatamente al procesarse, a diferencia de las versiones anteriores de Exchange que eran compatibles con el estándar MIME para correos electrónicos. Cuando Exchange Server 2007 envía y recibe a través de clientes que no pertenecen a MAPI, destruye las estructuras MIME del correo electrónico. Sin embargo, los mensajes codificados PGP/MIME son completamente compatibles con esta transición de Microsoft, incluso cuando MAPI no está en uso. Todos los mensajes enviados entre los clientes de MAPI de PGP Corporation también son totalmente compatibles.

Tenga en cuenta que los mensajes codificados que utilizan el formato de elemento heredado "PGP particionado" no siempre mostrarán el contenido de los mensajes HTML adecuadamente, y es posible que los conjuntos de caracteres extranjeros en estos mensajes no se reproduzcan correctamente cuando se procesan a través de Exchange Server 2007. Si estos mensajes se procesan desde clientes que no pertenecen a MAPI, el servidor puede borrar algunas partes del cuerpo del mensaje HTML encriptado y quitar información del conjunto sin caracteres ASCII. Por lo tanto, se generan mensajes que no preservan la fidelidad total. Si su organización utiliza la codificación de PGP particionado heredada con clientes que no pertenecen a MAPI, PGP Corporation no recomienda actualizar a Exchange Server 2007 en este momento. PGP Corporation está trabajando junto a Microsoft para buscar soluciones adicionales de compatibilidad entre Exchange Server y el estándar MIME.

PGP Corporation actualizará el Artículo 713 de la Base de conocimientos de soporte técnico a medida que vaya obteniendo más información.

Compatibilidad con el cliente de mensajería instantánea

PGP Desktop es compatible con los siguientes clientes de mensajería instantánea al encriptar mensajes instantáneos de AIM, transferencias de archivos y conexiones directas:

- AOL AIM 6.5.5
  - Para encriptar mensajes instantáneos con AIM 6.5, debe cambiar el puerto predeterminado que usa AIM de 493 a 5190.
  - Las conexiones de audio y video no están encriptadas por PGP Desktop.
  - La interoperabilidad continuada con el servicio AIM puede verse afectada por los cambios realizados en los protocolos AIM subyacentes después de que se lance PGP Desktop versión 10.0.
- Trillian 3.1 (Basic y Pro)

Otros clientes de mensajería instantánea pueden funcionar para mensajería instantánea básica, pero no se han certificado para su uso.

Compatibilidad de software antivirus para Windows

En todos los programas antivirus, habilitar el análisis en tiempo real detecta cualquier virus mientras se abren los correos electrónicos o los archivos adjuntos. Por lo tanto, si bien se recomienda deshabilitar la exploración de correo electrónico en algunos productos enumerados a continuación, su correo electrónico aun se analizará y usted tendrá la protección del producto antivirus contra los virus propagados por correo electrónico.

BitDefender Internet Security

- Cuando utiliza SMTP, POP o IMAP, deshabilite la función Protección en tiempo real o desinstale BitDefender. [13687]

Computer Associates eTrust EZ-Antivirus 7.x

- El análisis selectivo no es compatible con PGP Desktop.

Computer Associates Internet Security Suite 2007

- Es te producto no es compatible con PGP Desktop y no debe instalarse en el mismo sistema que PGP Desktop. [12023]

F-Secure AntiVirus, F-Secure Internet Security

- Deshabilitar la opción para analizar y eliminar virus del tráfico web en la configuración de F-Secure. Para obtener más información, consulte el Artículo 1767 de la Base de conocimientos de soporte técnico para PGP.

McAfee Internet Security Suite 2006, McAfee Internet Security Suite 2005, McAfee Internet Security 8.0, McAfee VirusScan 8.x hasta 10.x

- Si la exploración de correo electrónico está habilitada, PGP Desktop no procesará el correo electrónico. Deshabilite la exploración de correo electrónico del producto McAfee y habilite al análisis en tiempo real.
- No hay requisitos de configuración especiales adicionales para el correo electrónico MAPI.
- Cuando utilice McAfee VirusScan Enterprise 8.0i, deshabilite **Impedir que los gusanos de correo masivos envíen correo** en el cuadro de diálogo **Propiedades de protección de acceso** de la consola VirusScan. Si esta opción está habilitada, el correo electrónico SMTP se bloqueará. Para deshabilitar esta opción, haga clic con el botón secundario en el icono McAfee de la bandeja del sistema y elija Consola VirusScan. Haga doble clic en **Protección de acceso**. En el cuadro de diálogo **Protección de acceso**, debajo de **Puertos para bloquear**, anule la selección del cuadro para **Impedir que los gusanos de correo masivos envíen correo** (esta opción está habilitada de manera predeterminada).
- Al utilizar McAfee Security Center 9.3, el correo electrónico no será procesado por PGP Desktop. Detenga y deshabilite el servicio de proxy de McAfee. Con eso se deshabilitará la Protección de información personal de McAfee y el Control para padres, pero el proxy de correo electrónico de PGP podrá procesar los mensajes de correo.

Panda Platinum 2005 Internet Security 9.x

- No se requiere configuración especial.

Antivirus Sophos

- No se requiere configuración especial.

Symantec Norton AntiVirus 11.x hasta 12.x, Symantec Norton Internet Security 2005, Symantec Norton Internet Security 2006

- No se requiere configuración especial para el correo electrónico MAPI.
- Cuando utilice correo electrónico POP, habilite la opción **Protección automática** y deshabilite **Filtro de correo no deseado** y **Exploración de correo electrónico**. **Protección automática**, que está activada de manera predeterminada, proporciona protección contra los virus que se encuentran al abrir los mensajes de correo electrónico.
- Deshabilitar SSL/TLS en Configuración del servidor en PGP Desktop o PGP Universal Satellite. (En PGP Desktop, seleccione el cuadro de control Mensajería de PGP y elija **Mensajería > Editar la configuración del**

servidor. Para **SSL/TLS**, seleccione **No intentar**. En PGP Universal Satellite, en la ficha **Políticas**, seleccione **Ignorar SSL/TLS**). Estas versiones de Norton AntiVirus evitan que todos los clientes de correo electrónico utilicen SSL/TLS, independientemente del uso del software PGP.

Symantec Norton AntiVirus 9.x hasta 10.x, Symantec Norton Internet Security 2003, Symantec Norton Internet Security 2004

- Deshabilitar la exploración de correo electrónico.
- Para los usuarios de Norton Internet Security, deshabilitar **Control de Privacidad de Norton** y **Alerta de correo no deseado**.
- Deshabilitar SSL/TLS en Configuración del servidor en PGP Desktop y PGP Universal Satellite. (En PGP Desktop, seleccione el cuadro de control Mensajería de PGP y elija **Mensajería > Editar la configuración del servidor**. Para **SSL/TLS**, seleccione **No intentar**. En PGP Universal Satellite, en la ficha **Políticas**, seleccione **Ignorar SSL/TLS**). Estas versiones de Norton AntiVirus evitan que todos los clientes de correo electrónico utilicen SSL/TLS, independientemente del uso del software PGP.

Trend Micro Antivirus 12.x, Trend Micro PC-cillin Internet Security 2005

- No se requiere configuración especial.

Compatibilidad con cortafuegos personales

PGP Desktop para Windows se ha probado con los siguientes software de cortafuegos personales:

- **Zone Alarm:** el cortafuego Zone Alarm, de manera predeterminada, restringe el acceso al host local. Debido a que PGP Desktop vuelve a dirigir las conexiones al host local, esto impide que PGP Desktop funcione correctamente. Para solucionar esto, agregue el host local (127.0.0.1) como una dirección IP confiable en Zone Alarm (en la pantalla Firewall/Zones). El envío de correos electrónicos a través de proxy de PGP Desktop funcionará normalmente una vez que se realice esta acción. [6446]
- **Cortafuego personal CyberArmor:** PGP Desktop 10.0 no es compatible con las versiones 2.6.050802, 3.2.050802 ni anteriores del cortafuego personal InfoExpress CyberArmor. Antes de instalar PGP Desktop, debe actualizar estas versiones: para obtener más información, comuníquese con la línea de ayuda o con el proveedor (InfoExpress en support@infoexpress.com). [7010]
- **Webroot Desktop Firewall**: PGP Desktop es compatible sólo con la versión 5.8 de Webroot Desktop Firewall. Las versiones anteriores del software de Webroot no son compatibles con PGP Desktop.

Compatibilidad con Citrix y servicios de terminal

PGP Desktop para Windows se ha probado con el siguiente software de servicios de terminal:

- Citrix Presentation Server 4.0
- Citrix Metaframe XP
- Servicios de terminal de Windows 2003

Las siguientes funciones de PGP Desktop para Windows están disponibles en estos entornos, según se especifica:

- La encriptación de correo electrónico es totalmente compatible.
- La funcionalidad de PGP Zip es totalmente compatible.
- La funcionalidad de PGP Shred es totalmente compatible.
- PGP NetShare es totalmente compatible.
- PGP Virtual Disks no se puede montar en una letra de unidad en Citrix/TS, pero se puede montar en puntos de montaje del directorio en volúmenes NTFS.
- PGP Whole Disk Encryption no es compatible.
- Las tarjetas inteligentes no son compatibles.

Para obtener información sobre cómo instalar PGP Desktop en un servidor Citrix, consulte el Artículo 832 de la Base de conocimientos de soporte técnico para PGP.

Tarjetas inteligentes y tokens compatibles para autenticación de PGP WDE BootGuard

Esta sección describe los requisitos del sistema (tokens, lectores y tarjetas inteligentes compatibles).

Lectores de tarjetas inteligentes compatibles para la autenticación de PGP WDE

Los siguientes lectores de tarjetas inteligentes son compatibles cuando se comunican con una tarjeta inteligente en un momento previo al arranque. Estos lectores pueden utilizarse con cualquier tarjeta inteligente extraíble que sea compatible (no es necesario utilizar la misma marca de tarjeta inteligente y de lector).

Lectores de tarjetas inteligentes genéricas

La mayoría de los lectores de tarjetas inteligentes CCID son compatibles. Los siguientes lectores han sido probados por PGP Corporation:

- USB OMNIKEY CardMan 3121 para sistemas de escritorio (076b:3021)
- USB OMNIKEY CardMan 6121 para sistemas móviles (076b:6622)
- Lector USB 2.0 ActivIdentity (09c3:0008)
- Modelo SCR3311 de lector de tarjeta inteligente SCM Microsystem

Lectores de tarjetas inteligentes CyberJack

- Teclado numérico Reiner SCT CyberJack (0c4b:0100).

Lectores de tarjetas inteligentes ASE

- Lector USB Athena ASEDrive IIIe (0dc3:0802)

Lectores de tarjetas inteligentes incrustados

- Lector incrustado Dell D430
- Lector incrustado Dell D630
- Lector incrustado Dell D830

Tarjetas inteligentes o tokens compatibles para autenticación de PGP WDE

PGP Whole Disk Encryption es compatible con las siguientes tarjetas de autenticación previa al arranque:

- Tarjetas ActiveIdentity ActivClientCAC, modelo 2005
- Aladdin eToken PRO 64 K, de 2048 bits compatible con RSA
- Aladdin eToken PRO con llave USB 32 K, de 2048 bits compatible con RSA
- Aladdin eToken PRO sin capacidad de 2048 bits (tarjetas inteligentes anteriores)
- Aladdin eToken PRO Java 72 K
- Aladdin eToken NG-OTP 32 K

> **Nota:** otros Aladdin eTokens,como tokens con flash, deberían funcionar siempre que sean compatibles con APDU y con tokens compatibles. Las versiones OEM de Aladdin eTokens, como aquellas lanzadas por VeriSign, deberían funcionar siempre que sean compatibles con APDU y con tokens compatibles.

- Token USB de criptografía Athena ASEKey para Microsoft ILM
- Tarjeta inteligente de criptografía Athena ASECard para Microsoft ILM

> **Nota:** los tokens Athena son compatibles únicamente para el almacenamiento de credenciales.

- Axalto Cyberflex Access 32K V2
- Tarjeta inteligente Charismathics CryptoIdentity plug 'n' crypt
- EMC RSA SecurID SID800 Token (versión 1 y 2)

> **Nota:** este token es compatible únicamente para el almacenamiento de llaves. SecurID no es compatible.

- Tarjeta inteligente EMC RSA 5200

- Marx CrypToken USB token
- Rainbow iKey 3000
- Tarjeta inteligente S-Trust StarCOS

  Nota: las tarjetas S-Trust SECCOS no son compatibles.

- Token USB SafeNet iKey 2032
- Tarjeta inteligente Telesec NetKey 3.0 de T-Systems
- Tarjeta inteligente TCOS 3.0 IEI de T-Systems

Tarjetas de verificación de identidad personal (PIV)

- Tarjetas de verificación de identidad personal Oberthur ID-One Cosmo V5.2D con el software de cliente ActivClient versión 6.1.
- Tarjetas de verificación de identidad personal Sm@rtCafe Expert 3.2 Giesecke and Devrient con el software de cliente ActivClient versión 6.1.

Instrucciones de instalación

Para instalar PGP Desktop en su sistema de Windows

1. Ubique y haga doble clic en la aplicación de instalador de PGP Desktop.
2. Siga las instrucciones en pantalla.
3. Si se le solicita, reinicie el sistema.

Para obtener información adicional, incluidas las instrucciones de actualización, consulte la *Guía del usuario de PGP Desktop para Windows*.

Licencia

PGP Desktop utiliza un sistema de licencias para determinar qué características estarán activas. Según la licencia que tenga, se activan algunas o todas las funciones de PGP Desktop. Consulte a su administrador de PGP si tiene preguntas sobre las funciones que están disponibles con su licencia.

Utilice el Asistente de instalación para ingresar la licencia de PGP Desktop después de la instalación. Si se encuentra en un dominio protegido por PGP Universal Server, el administrador de PGP puede haber configurado su instalador de PGP Desktop con una licencia.

Las funciones de PGP Desktop que estarán activas en su sistema dependerán del tipo de licencia que usted tenga:

- PGP Desktop Professional 10.0 incluye PGP Desktop Email y PGP Whole Disk Encryption
- PGP Desktop Storage 10.0 incluye PGP Whole Disk Encryption y PGP NetShare.
- PGP Desktop Enterprise 10.0 incluye PGP Desktop Email, PGP Whole Disk Encryption y PGP NetShare.

También puede utilizar PGP Desktop sin licencia, pero *sólo para usos no comerciales*. El uso comercial de PGP Desktop sin licencia es una infracción del Contrato de licencia de usuario final (EULA). Si decide utilizar PGP Desktop sin licencia (y tiene permiso legal de uso no comercial en virtud de EULA), la mayoría de las funciones de PGP Desktop no funcionarán. Sólo las funcionalidades básicas estarán disponibles.

Para obtener más información sobre las opciones de compra y licencia de PGP Desktop, visite la Tienda PGP.

Información adicional

General

- **Caracteres japoneses y procesamiento de Ventana actual y Portapapeles:** las funciones de encriptación y desencriptación de Ventana actual y Portapapeles no son compatibles con ISO-2022-JP. [7489]
- **Compatibilidad con aplicaciones Oracle**: si tiene problemas con la aplicación Oracle con Oracle JInitiator, quizá pueda utilizar la última versión de Sun Java Runtime Environment para ejecutar sus aplicaciones Oracle.

[15543]

- **Compatibilidad con Google Desktop**: PGP Desktop es compatible con el software Google Desktop instalado si deshabilita la opción en Google Desktop para indexar el correo. Para obtener más información, consulte el Artículo 958 de la Base de conocimientos de soporte técnico para PGP. [16286, 18499]
- **Cambios de la contraseña de Windows:** PGP Desktop depende de la API de protección de datos (DPAPI) de Microsoft para asegurar los datos de enrolamiento del usuario. Los usuarios de Windows XP SP2 pueden dejar de tener acceso a la información de enrolamiento debido a un problema conocido en SP2. Los usuarios afectados por este problema de Microsoft deben actualizar a Windows XP SP3 y volver a enrolarse. Para obtener más información, consulte el Artículo 890951 de Microsoft Knowledge Base. [20852]
- **Cambios de la contraseña de Windows**: Para garantizar el funcionamiento correcto de varias funciones de PGP, entre ellas SSO y las llaves SKM, las contraseñas de Windows no se deben cambiar mediante el comando "net user" del símbolo del sistema de Windows. [22825]

Llaves PGP

- **RSA SecurID SID800**: RSA SecurID SID800 sólo admite SHA-1. Al generar una llave en RSA SecurID SID800, modifique las propiedades de la llave haciendo clic en el botón Avanzado y en Hashes seleccione sólo SHA-1. Si ya se ha generado una llave, obtenga las Propiedades de llave, edite el conjunto de Hashes compatibles y seleccione sólo SHA-1. [14861]
- **Tarjetas inteligentes GemPlus**: las tarjetas inteligentes sólo admiten SHA-1. Al generar una llave en las tarjeta inteligentes GemPlus, modifique las propiedades de la llave haciendo clic en el botón Avanzado y en Hashes seleccione sólo SHA-1. Si ya se ha generado una llave, obtenga las Propiedades de llave, edite el conjunto de Hashes compatibles y seleccione sólo SHA-1. [15681, 16603]
- **Tokens Athena**: Al crear llaves PGP de 2048 bits que se utilizarán con tokens Athena, no puede copiar la llave PGP al token. Sin embargo, puede crear la llave de 2048 bits directamente en el token. [24861]

Mensajería de PGP

- **Correo electrónico Thunderbird enviado a usuarios de BlackBerry**: si el cliente de correo electrónico Thunderbird está configurado para enviar correos electrónicos sólo en formato HTML y el mensaje se encripta con PGP Universal Server o PGP Desktop antes de que llegue a la puerta de enlace BES, el destinatario no podrá visualizar el mensaje de correo electrónico en su BlackBerry. Para solucionar este problema, configure el cliente de correo electrónico Thunderbird para que no envíe mensajes HTML solamente. [16273]
- **Políticas de MAPI y mensajes:** las políticas basadas en el estado "El mensaje está <x>" no son compatibles con MAPI actualmente. [9448]
- **Mensajes heredados encriptados a conjuntos de caracteres no romanos**: la funcionalidad de desencriptación de **Ventana actual** y **Portapapeles** se ha mejorado para detectar errores de conversión en el conjunto de caracteres UTF-8. En ese caso, el contenido se desencriptará a la página de códigos local del sistema. Tenga en cuenta que los mensajes heredados de la versión 8 de PGP Desktop e inferiores no eran compatibles con la identificación de conjuntos de caracteres adecuada. Por lo tanto, posiblemente la página de códigos local no sea correcta. Si se encuentra con mensajes heredados de este tipo que se están desencriptando a un conjunto de caracteres incorrecto desde el portapapeles, es posible que necesite utilizar herramientas de terceros para convertir el conjunto de caracteres resultante al conjunto correcto. [11889, 19679]
- **PGP Desktop 8.x y caracteres internacionales:** tenga en cuenta que PGP Desktop 8.x no era compatible con caracteres internacionales en el contenido del cuerpo del mensaje. Para utilizar otros idiomas diferentes al inglés en el contenido de los mensajes, asegúrese de que los remitentes estén utilizando PGP 9.0.0 o una versión superior. Es posible que algunas veces pueda hacer que PGP Desktop 8.x o una versión inferior cree un mensaje adecuado al forzar el uso del conjunto de caracteres UTF-8. [11257, 11888]
- **Agregar comentarios a los mensajes seguros:** para garantizar la visualización adecuada de los comentarios agregados a los mensajes seguros con la opción **Agregar un comentario a los mensajes seguros**, PGP Corporation recomienda utilizar texto ASCII en el campo Comentario. [11127]
- **Mensajes S/MIME:**
    - **Mensajes de correo electrónico firmados S/MIME:** la mensajería de PGP no puede procesar los correos electrónicos firmados S/MIME si el certificado de firma X.509 no está incluido en el correo electrónico. Casi siempre se incluye el certificado en el correo electrónico, a menos que el remitente desactive esta opción. Si el mensaje no está procesado con PGP, aún puede procesarse con la aplicación del cliente de correo. [9489, 9491]

- **S/MIME y MAPI:** los usuarios S/MIME que desean utilizar S/MIME con MAPI deben asegurarse de que haya un certificado X.509 añadido en las llaves, de lo contrario, es posible que PGP Desktop no pueda procesar estos mensajes cuando se guarden en la carpeta de elementos enviados. [9858]

- **Microsoft Outlook:**
  - **Microsoft Outlook**: los mensajes que se han procesado con PGP Desktop no pueden modificarse desde la bandeja de salida de Microsoft Outlook. [20269]
  - **Microsoft Outlook y ESET Antivirus**. Al utilizar Microsoft Outlook en un sistema que tiene instalado ESET Antivirus, es posible que Outlook demore en abrirse. [22192]
  - **Usuarios MAPI/Exchange y objetos en línea:** si usted es un usuario MAPI/Exchange y está enviando mensajes con contenido incrustado en un formato exclusivo (objetos en línea), PGP Desktop asegurará el mensaje completo. Esto hará que sólo los destinatarios de un entorno MAPI/Exchange puedan leer y visualizar los objetos en línea. [5530]
  - **Outlook MAPI:** si está utilizando Outlook en un entorno MAPI, utilice el registro de PGP para confirmar la validez de las anotaciones de la firma de PGP en los cuerpos de los mensajes, a menos que el mensaje se haya desencriptado con su PGP Universal Server, que hará esto por usted. [6819, 7304]
  - **Outlook Connector para Notes:** no es compatible con Outlook Connector para Notes, que le permite a un cliente Outlook emular un cliente de Lotus Notes. [7567]
  - **Correo electrónico MAPI en Windows Vista**: después de actualizar Windows XP a Windows Vista sin reinstalar PGP Desktop, los mensajes MAPI se envían sin encriptar y los mensajes existentes encriptados no se desencriptan. Cuando actualiza su sistema operativo a Windows Vista, PGP Corporation recomienda que primero desinstale PGP Desktop, actualice su sistema y reinstale PGP Desktop. [13119]
  - **Correo electrónico MAPI en los sistemas Windows 2008 Server R2**: PGP Desktop Email no funciona con los sistemas Windows 2008 Server R2 a menos que la clave de registro `RequireSignedAppInit_DLLs` se establezca en `0` (que se encuentra en HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows). Para obtener más información, consulte el artículo de Microsoft MSDN AppInit_DLLs en Windows 7 y Windows Server 2008 R2. [25507]
- **Lotus Notes:**
  - **Lotus Notes y usuarios deshabilitados:** cuando se ha deshabilitado un usuario, el correo electrónico enviado se bloquea inicialmente. Para solucionar este problema, envíe el correo electrónico nuevamente y se enviará sin encriptar, como se espera. [12234]
  - **Lotus Notes y usuarios deshabilitados:** cuando se ha deshabilitado un usuario y se ha habilitado nuevamente, el usuario debe reiniciar Lotus Notes para enviar correos electrónicos encriptados. [12236]
  - **ID de notas japonesas**: debido al modo en que Lotus Notes crea direcciones SMTP desde la Id. de usuario, las cuentas con Id. de usuarios japoneses pueden mostrarse de forma incorrecta o truncarse en algunos cuadros de diálogo de PGP Desktop. Esto no interfiere con el funcionamiento de PGP Desktop ni con la entrega del correo electrónico del usuario. [12913]
- **POP:** las cuentas POP de Verizon arrojan una respuesta incorrecta al conectarse a los puertos POP/SMTP si no ha adquirido los servicios Silver o Gold de Verizon. En este caso, debe configurar los puertos manualmente a 110/25 en la política de interfaz de usuario para la cuenta, respectivamente, a fin de evitar la conexión a los puertos normales. [NBN]
- **SMTP:** active la autenticación SMTP en el cliente de correo electrónico si no está activada actualmente. [NBN]
- **Cambios de licencia de mensajería de PGP:** si cambia la licencia de PGP Desktop de una licencia que *no* es compatible con la funcionalidad de mensajería de PGP (por ejemplo, PGP Whole Disk Encryption para empresas) a una licencia que *sí* es compatible con la mensajería de PGP, debe detener y reiniciar los servicios de PGP una vez que la nueva licencia esté aceptada. Esto garantiza que PGP Desktop pueda proteger sus mensajes de manera adecuada. Para detener los servicios de PGP, haga clic en el icono de PGP Tray y elija **Salir de servicios de PGP**. Para reiniciar los servicios, elija **Inicio > Programas > PGP > PGP Desktop**. [8107, 12200]
- **Mensajería instantánea:**
  - **Conexiones AIM múltiples:** Si el sistema tiene maneras múltiples de acceder al servicio AIM (por ejemplo, accesos LAN e inalámbricos) y se pierde la conexión con AIM, pero el servidor AIM no reconoce la pérdida de conexión y el cliente MI accede al servicio AIM nuevamente con el otro acceso a la red, el servidor AIM verá que usted ha iniciado sesión a la misma cuenta AIM desde dos lugares. Esto hará que

PGP Desktop deshabilite el proxy de AIM por el estado de error, y el servidor AIM mostrará un mensaje que le dirá que la sesión de su cuenta se ha iniciado desde dos ubicaciones diferentes. Para resolver este problema, simplemente responda el mensaje desde el servidor AIM con 1. La sesión AIM anterior se suspenderá, y PGP Desktop encriptará la sesión AIM restante. [NBN]

- **Compatibilidad con AIM 6.5**: PGP Desktop no asegura los mensajes instantáneos cuando la versión en inglés (lanzada) de AIM 6.5 se ejecuta en sistemas operativos Windows XP o Windows Vista de 64 bits, o en cualquier sistema operativo alemán o japonés. [16393]

PGP NetShare

- **Compatibilidad con SmartFTP**: SmartFTP de SmartSoft Ltd. no puede utilizarse para descargar archivos a una carpeta protegida por PGP NetShare. En su lugar, use el cliente FTP incorporado en Windows. [17942]
- **Vínculos de Windows**. PGP NetShare no sigue los vínculos de Windows (archivos `.lnk`), incluidos los vínculos como "Mis sitios de red". Agregar una carpeta a PGP NetShare que en realidad es un vínculo protegerá el archivo del vínculo y no la ubicación deseada. [13339]
- **Utilización de PGP NetShare con Windows Vista:** en los sistemas Windows Vista, el método arrastrar y colocar no es compatible para agregar carpetas nuevas a una carpeta protegida de PGP NetShare. Este problema no ocurre con Windows Vista SP1. [12506]
- **Utilización de PGP NetShare con Windows Vista de 64 bits:** la ficha de propiedades de PGP NetShare no está disponible en las versiones Windows Vista de 64 bits. [17622]
- **Incompatibilidad del software con la función PGP NetShare:** los siguientes programas no son compatibles con PGP NetShare:
  - Securewave Sanctuary Device Control 3.0.3. Para usar PGP Desktop con Sanctuary Device Control, es necesario actualizar el software de Securewave a la versión 4.1 o superior. [12850]
  - CommVault System Data Migrator. Para usar PGP Desktop con Data Migrator, es necesario eliminar del registro PGP NetShare DLL (en el símbolo del sistema, escriba `regsvr32 /u PGPfsshl.dll`). [12016]
- **Aplicaciones en lista blanca**: las aplicaciones en lista blanca son aplicaciones que el administrador de PGP Universal Server ha definido para que todos los archivos creados por la aplicación se encripten obligatoriamente. Los archivos creados por estas aplicaciones en lista blanca se bloquean (requieren autenticación para tener acceso) después de cerrar sesión o cerrar el sistema. [17491]
- **Utilización de PGP NetShare y SharePoint con Windows Vista de 64 bits:** el menú de acceso directo de PGP NetShare no está disponible en las versiones Windows Vista de 64 bits cuando se visualiza una carpeta dentro de SharePoint. Para acceder al menú de acceso directo, visualice la carpeta con el explorador de Windows. [19421]

PGP Portable

- **Acceso a los datos en sistemas Windows 2000**. Al montar un disco de PGP Portable Disk en un sistema Windows 2000, los contenidos están disponibles sólo a través de un explorador web, y los datos son de sólo lectura. [21446]
- **PGP Portable y Microsoft Office 2003**. PGP Portable es compatible con Microsoft Office 2003 si Office Service Pack 3 está instalado. [21854]
- **PGP Portable y Microsoft Office 2003**. Los documentos de Microsoft Office 2003 no se pueden agregar a un disco PGP Portable si el disco se crea en un sistema Windows Vista. [21697]
- **Acceso a los datos en sistemas Windows XP**. Al montar un disco PGP Portable en Windows XP, se producirá el error "No conectado" si hay otro proceso que esté utilizando el puerto 80. [21869]
- **Creación de nuevos documentos de Word en un disco PGP Portable**. Al crear un nuevo archivo de Microsoft Word en un disco de PGP Portable Disk en Windows XP (hacer clic con el botón secundario en el disco montado de PGP Portable Disk y seleccionar **Nuevo > Archivo > Documento de Microsoft Word**), el archivo Word resultante de cero bytes es de sólo lectura. Para editar el archivo, guárdelo con un nuevo nombre (en el disco de PGP Portable Disk). [21680]
- **Incorporación de datos en sistemas Windows XP**. Para agregar datos a un disco PGP Portable en un sistema Windows XP, configure la política local **Permiso para formatear y expulsar el dispositivo extraíble** en **Administrador y usuarios interactivos**. [21975]
- **Requisitos de espacio en disco**. Al copiar archivos grandes a un disco PGP Portable, asegúrese de contar

con espacio suficiente en la unidad local. La cantidad de espacio necesaria es equivalente a la cantidad de datos que se copiarán en el disco PGP Portable. [21595]

- **Frases de contraseña de PGP Portable**: No se admite el uso de caracteres japoneses para las frases de contraseña al crear un nuevo disco de PGP Portable o al cambiar la frase de contraseña de un disco existente. [21717]
- **Nombres de archivo de un disco PGP Portable**. Al crear un disco PGP Portable, la combinación del nombre de archivo y de los nombres de carpeta no pueden exceder los 240 caracteres. [21816]
- **PGP Portable y Trend Micro Antivirus**. Para crear un disco de PGP Portable en sistemas Windows XP que ya tienen Trend Micro Antivirus instalado, detenga o desactive todos los servicios Trend Micro antes de crear el disco de PGP Portable. Puede iniciar o habilitar nuevamente los servicios después de que el disco se haya creado. Este problema no se produce en los sistemas Windows 7 de 64 bits. [26091]

PGP Shred

- **Trituración (borrado de archivos pequeños)**: la trituración de archivos pequeños (menores a 1 K) en algunos discos con formato NTFS puede dejar restos del archivo debido a una optimización de NTFS que almacena los datos del archivo en estructuras de datos internos para los archivos muy pequeños. Estas estructuras no se consideran espacio libre, ni siquiera después de eliminar el archivo y, por lo tanto, tampoco se triturarán con la función Espacio libre de PGP Shred, de PGP Desktop. Además, NTFS admite el Registrado en diario, que puede guardar los datos de archivos triturados en una caché del sistema operativo interna. Para obtener mayor seguridad de trituración en discos NTFS, recomendamos iniciar el sistema desde un sistema operativo en una partición diferente y utilizar la opción de PGP Desktop en la función Triturar espacio libre para sobrescribir estas estructuras de datos NTFS (la casilla de comprobación **Triturar estructuras de datos internos de NTFS**). Esto no afecta FAT32 ni otros sistemas de archivos compatibles. [NBN]
- **Trituración de archivos dispersos**: los archivos dispersos, comúnmente utilizados para las imágenes de disco, las instantáneas de la base de datos, los archivos de registro y las aplicaciones científicas, no pueden eliminarse de manera segura con PGP Shred. [21255]
- **Trituración automática**: la trituración automática al vaciar la papelera de reciclaje o la papelera no es compatible con el software de grabación de CD incorporado en Windows. [22794]

PGP Viewer

- **Lotus Notes**: dado el diseño de la arquitectura de Lotus Notes, un mensaje encriptado no se puede arrastrar desde el cliente de correo electrónico Lotus Notes y colocar en PGP Viewer para desencriptarlo. [23384]
- **Visualización de mensajes de correo electrónico de sólo firma con Shift-JIS**: Los mensajes de Outlook Express o Windows Mail firmados con Shift-JIS no se pueden verificar con PGP Viewer. Este problema no ocurre si el mensaje está encriptado y firmado. [22870]
- **Mensajes S/MIME**: Los mensajes encriptados con S/MIME no se pueden desencriptar con PGP Viewer en esta versión. [22022]
- **Visualización de mensajes desencriptados**: Si arrastra un elemento a PGP Viewer y el mensaje no aparece, reinicie PGP Viewer y arrastre el elemento nuevamente. [22215]
- **Copia de mensajes de correo electrónico a la bandeja de entrada**: Al copiar un mensaje de correo electrónico de Microsoft Outlook 2003 a la bandeja de entrada mediante PGP Viewer, la fecha y la hora del mensaje cambia, y se reemplaza por la fecha y la hora actual. [24355]
- **Visualización de correo electrónico de MAPI**: Los mensajes de Microsoft Outlook abiertos con PGP Viewer mostrarán Dirección sin coincidencia en el campo De: [24703]
- **Cómo cancelar la solicitud de frase de contraseña**: Si arrastra un elemento a PGP Viewer y hace clic en **Cancelar** cuando se le solicita la frase de contraseña, deberá reiniciar PGP Viewer nuevamente. Esto es necesario para que pueda escribir la frase de contraseña para desencriptar mensajes. [25390]
- **PGP Viewer con Outlook Express en los sistemas Microsoft Windows XP de 64 bits**: En los sistemas Microsoft Windows XP de 64 bits, no se puede utilizar la opción **Copiar a bandeja de entrada** después de arrastrar y soltar un mensaje en PGP Viewer si el programa de correo electrónico predeterminado es Outlook Express. [23815]

PGP Virtual Disk

- **Utilización con llaves basadas en certificados personales**: para montar un PGP Virtual Disk que está asegurado con una llave basada en un certificado personal, tenga en cuenta que no debe ingresar la frase de

contraseña cuando se le pida esto en el cuadro de diálogo Ingresar la frase de contraseña de PGP; en su lugar, haga clic en **Ingresar**. [14762]

- **PGP Virtual Disk de NTFS y Windows Vista**: es posible que los discos NTFS creados en Windows XP no puedan manejarse correctamente en Windows Vista. Para obtener mejores resultados, cree los discos NTFS en Windows Vista. Se espera que una próxima actualización de Microsoft resuelva este problema con Windows. [12644]

PGP Whole Disk Encryption

- **Compatibilidad con versiones anteriores**. Para acceder a los discos encriptados con esta versión de PGP WDE, solamente se puede utilizar la misma versión de PGP WDE para Mac OS X o la versión 9.9.0 (o versiones superiores) de PGP WDE para Windows. [19875]
- **Licencias de evaluación de PGP WDE**. Si utiliza PGP WDE con una licencia de evaluación en un entorno gestionado por PGP Universal Server, recuerde obtener una licencia válida *antes de* la fecha de caducidad de la licencia de evaluación. Esto evitará que el disco se desencripte de manera automática cuando caduque la licencia de evaluación. [16445]
- **Autenticación de PGP WDE**: la tarjeta inteligente ActiveIdentity ActivClientCAC modelo 2002 no es compatible con esta versión. Para utilizar la tarjeta ActiveClient CAC, use el modelo 2005. [16259]
- **Recuperación de frase de contraseña**: A los usuarios de tokens que utilizan la recuperación de frase de contraseña para la autenticación en PGP BootGuard se les solicitará que cambien la frase de contraseña. Esta solicitud se puede ignorar, dado que el PIN no cambiará aunque ingrese texto en el cuadro de diálogo o haga clic en **Cancelar**. [24335]
- **Recuperación de frase de contraseña**: La recuperación de frase de contraseña está disponible solamente para los discos de arranque encriptados. [24510]
- **Recuperación de frase de contraseña**: Si utiliza la opción **Olvidé mi frase de contraseña** en la pantalla de PGP BootGuard e ingresa un nombre de usuario incorrecto, deberá hacer clic en **Cancelar** para regresar a la pantalla de PGP BootGuard y seleccionar **Olvidé mi frase de contraseña** nuevamente. [24825]
- **PGP WDE y los lectores de tarjetas inteligentes**: Cuando utiliza un lector de tarjeta inteligente con un PIN pad (teclado para ingreso de código PIN) incorporado, es posible que no se acepte el PIN correcto la primera vez que lo ingrese en el teclado y deba ingresarlo nuevamente. Cuando aparece este mensaje, haga clic en Aceptar sin escribir nada. Esto permitirá la aceptación del PIN o transferirá el control al PIN pad del lector de tarjetas inteligentes, donde puede ingresar el PIN nuevamente. [16143]
- **PGP WDE y los lectores de tarjetas inteligentes**: La autenticación del arranque previo con un lector de tarjetas inteligentes no es compatible en los sistemas Panasonic Toughbook y Sony Vaio P-Series Mini. [20638]
- **PGP WDE y GemXpresso**: PGP Desktop no es compatible con la familia de tarjetas inteligentes GemXpresso. Las llaves de la tarjeta inteligente GemXpresso pueden utilizarse para encriptar las carpetas protegidas de PGP NetShare y PGP Virtual Disk, pero no pueden utilizarse para encriptar un disco o un disco extraíble. [16415]
- **Controladores USB de OHCI**: PGP BootGuard no funciona actualmente con los controladores USB de OHCI. En consecuencia, los tokens no funcionan en PGP BootGuard, en esos sistemas. [15800]
- **Encriptación de unidades:** Las unidades con un tamaño de sector que no sea de 512 bytes no son compatibles con PGP WDE y no se pueden encriptar. [21126]
- **PGP WDE y SSO**: si tiene problemas para sincronizar el cambio de una contraseña de Windows en un sistema Windows XP, siga los pasos a continuación para solucionar el problema: [17269]
    1. En el escritorio de Windows, haga clic con el botón secundario en Mis sitios de red y seleccione **Propiedades** en el menú de acceso directo.
    2. Seleccione **Avanzado > Configuración avanzada**.
    3. Seleccione la ficha **Orden de proveedores**.
    4. Vuelva a organizar el orden de los proveedores de manera que `PGPpwflt` se encuentre arriba de la tarjeta Intel.
    5. Haga clic en **Aceptar**.

    También puede modificar el archivo de instalación .msi. Utilice el comando `PGP_SET_HWORDER=1` para colocar PGPpwflt en el primer lugar de la lista. Por ejemplo, ejecute el archivo de instalación .msi con el siguiente comando:

    ```
    msiexec /i pgpdesktop.msi PGP_SET_HWORDER=1
    ```

- **PGP WDE SSO en redes Novell**: la función Single Sign-On (Inicio de sesión único) de PGP WDE no funciona en sistemas Windows Vista con el cliente de redes Novell. Una vez que se ha autenticado en la pantalla de PGP Bootguard, deberá ingresar su contraseña nuevamente para iniciar Windows Vista. [16688]
- **PGP WDE SSO en redes Novell**: cuando utiliza la función Single Sign-On (Inicio de sesión único) de PGP WDE en sistemas Windows Vista con el cliente de redes Novell, los usuarios fuera de línea reciben un mensaje de seguridad de Novell que indica que "no pudo encontrarse el árbol o servidor". Para continuar el inicio de sesión en Windows, haga clic en Sí, y el inicio de sesión continúa normalmente. [16995]
- **Compatibilidad con TPM**: estamos validando muchas implementaciones de TPM diferentes. Nos interesan los resultados de sus pruebas de cualquier otro sistema TPM adicional. [14666]
- **Autenticación de token**: para la autenticación de token en PGP BootGuard, es necesario presionar CTRL+ENTER en lugar de Enter. Es posible que se produzca una demora durante la autenticación de tokens en PGP BootGuard. [14792, 16466]
- **PGP WDE y Autenticación de dos factores USB**: si ha creado un usuario de frase de contraseña con una unidad USB flash y ha encriptado el disco de arranque, es posible que al reiniciar no se reconozca su dispositivo USB en la pantalla de PGP BootGuard. Sin embargo, aún puede autenticar en la pantalla de PGP BootGuard utilizando solamente la frase de contraseña. Si desea usar la autenticación de dos factores, deberá desencriptar su disco, crear otra frase de contraseña con otro dispositivo USB y encriptar nuevamente el disco de arranque. [16577]
- **Discos externos y Autenticación de dos factores**: si ha encriptado un disco externo tanto con un usuario de frase de contraseña como con un usuario de token, debe insertar el token antes de conectar el disco externo. [19013]
- **Tarjetas inteligentes Aladdin**: las tarjetas inteligentes Aladdin no generan de manera adecuada las llaves de 2048 bits con la versión 4.5.52 del software Aladdin. Estas llaves no pueden utilizarse para la autenticación del arranque previo de PGP WDE. PGP Corporation está trabajando con Aladdin para solucionar este problema. Tenga en cuenta que los tokens de Aladdin no tienen este problema. [16699]
- **Tarjetas de criptografía Athena ASECard:** la tarjeta de criptografía Athena ASECard no es compatible con los lectores OmniKey para la autenticación del arranque previo. Utilice un lector compatible diferente con las tarjetas inteligentes Athena para la autenticación del arranque previo.[18283]
- **Actualización**: la pantalla de PGP BootGuard no se actualiza inmediatamente después de que se actualiza a PGP Desktop 10.0. Para visualizar la pantalla de PGP BootGuard actualizada (con las nuevas opciones de teclado y de inicio de sesión), reinicie el sistema por segunda vez. [NBN]
- **Encriptación de una unidad extraíble:** algunos tipos de dispositivos flash extraíbles no pueden encriptarse con el formato proporcionado por el proveedor. Deben formatearse en Windows antes de encriptarse. [12362]
- **Encriptación de una unidad extraíble**: si **Encriptar automáticamente el disco de arranque en la instalación** y **Forzar la encriptación del disco extraíble** están permitidas por la política, puede encontrar un error al insertar un disco USB mientras se encripta un disco fijo. Para resolver este problema, espere hasta que se haya terminado el proceso de encriptación en el disco fijo. [12167]
- **PGP WDE e Hibernación:** cuando se reanuda el sistema del modo Hibernación, es posible que aparezca una solicitud de contraseña de dominio adicional, incluso si la función Single Sign-on (Inicio de sesión único) está activa. [9935]
- **Utilización de discos extraíbles protegidos por PGP WDE con PGP Desktop 9.x y 10.0:** los discos encriptados con PGP Desktop 9.0, 9.5 ó 9.6 pueden utilizarse en un sistema PGP Desktop 9.7 o superior y funcionar sin problemas. Sin embargo, si hace algún cambio en el disco con el software PGP Desktop 9.5 ó 9.6 (como cambiar la frase de contraseña, agregar o eliminar usuarios, etcétera), el disco dejará de funcionar en el sistema PGP Desktop 9.0. [11610, 11845]
- **Recuperación del disco:** como una buena práctica, si debe realizar una actividad de recuperación de disco en un disco protegido con Whole Disk Encryption (WDE) (Encriptación de disco completo [WDE]), PGP Corporation recomienda que primero desencripte el disco (utilizando la opción **Disco PGP Desktop > Desencriptar** o el disco de recuperación PGP WDE preparado, o conectando el disco duro a través de un cable USB a otro sistema y desencriptándolo desde el software PGP Desktop de ese sistema). Una vez que el disco se haya desencriptado, comience con las actividades de recuperación. [NBN]
- **Utilización de PGP WDE con Norton Ghost 9 ó 10:** Ghost es compatible con discos completamente encriptados. Algunas veces, Ghost expone errores cuando se utiliza para realizar copias de respaldo de discos encriptados parcialmente en sistemas operativos Windows. Para recuperarse de un error como este, reinicie el sistema y realice un Windows chkdsk cuando se reinicie el sistema. Ghost debería funcionar nuevamente.

[13004]

- **Compatibilidad de las versiones anteriores de los discos de recuperación de PGP WDE:** los discos de recuperación de PGP WDE sólo son compatibles con la versión de PGP Desktop con la que fueron creados. Por ejemplo, si intenta utilizar un disco de recuperación 9.0.x para desencriptar un disco protegido con la versión de PGP WDE 9.5 o superior, el disco PGP WDE se vuelve inutilizable. [10556]
- **Preparación para la encriptación del disco:** los errores que se generan cuando intenta encriptar su disco a menudo son provocados por sectores dañados del disco duro. Estos pueden corregirse frecuentemente con productos de terceros que pueden reparar el disco y asegurar sus buenas condiciones. El programa CHKDSK de Windows puede resolver el problema en algunos casos, pero a veces se necesitan programas más globales, como SpinRite de Gibson Research Corporation (http://www.grc.com). Además, si el disco está muy fragmentado, PGP Corporation recomienda desencriptar el disco antes de realizar la encriptación con el Desfragmentador de disco de Windows. [10561]
- **PGP WDE y diagnósticos de sistemas de arranque Dell:** (sólo en sistemas Dell) los diagnósticos de los sistemas de arranque avanzados a los que normalmente se puede acceder presionando F12 durante el proceso de arranque no están disponibles en los discos encriptados con PGP WDE. Para ejecutar los diagnósticos de arranque avanzados con F12, primero desencripte el disco y ejecute los diagnósticos. [12120]
- **Incompatibilidad del software con la función PGP Whole Disk Encryption:** algunos programas no son compatibles con la función PGP Whole Disk Encryption. No instale este producto en un sistema con PGP Desktop y no instale PGP Desktop en un sistema con estos productos:
  - Faronics Deep Freeze (cualquier edición) [15443]
  - Utimaco Safeguard Easy 3.x [8010]
  - Productos de encriptación del disco duro de GuardianEdge Technologies: Encryption Anywhere Hard Disk y Encryption Plus Hard Disk, anteriormente denominados productos PC Guardian. [12005, 12065]
  - Safeboot Solo coexiste en el sistema, pero bloquea PGP WDE.
  - SecureStar SCPP coexiste en el sistema, pero bloquea PGP WDE.
  - Dell Embassy Trust Suite de Wave Systems coexiste en el sistema, pero lo vuelve más lento. [19297]
- **Tokens de recuperación de PGP WDE:** en un entorno gestionado por Universal, si un disco se encripta con PGP Whole Disk Encryption antes de enrolarse con PGP Universal, la opción **Encriptar automáticamente el disco de arranque en la instalación** debe estar seleccionada en PGP Universal Server para que el token de recuperación del disco completo (WDRT) se cargue en PGP Universal Server. De lo contrario, no se cargará automáticamente el token cuando se enrole el sistema con PGP Universal. [12183]
- **IBM Fingerprint Software:** PGP Desktop es compatible con la versión 5.6.1 o superior de ThinkVantage Fingerprint Software de IBM. [13786]
- **PGP WDE SSO**: cuando utiliza PGP WDE SSO, PGP Corporation recomienda que las organizaciones habiliten la política de grupo de Microsoft **Esperar siempre la red al inicio de la computadora e inicio de sesión**. Esto garantiza que los cambios de caducidad de la contraseña y los cambios forzados ocurran tan pronto como sea posible. Para obtener más información sobre esta configuración, consulte los siguientes artículos de la Microsoft Knowledge Base. [14142]
  - http://technet.microsoft.com/en-us/library/bb456994.aspx
  - http://support.microsoft.com/kb/305293
- **Modificación de la partición del sistema**: no realice ningún cambio en la partición del sistema de un disco de arranque que haya sido encriptado con PGP WDE, si lo hace, el próximo arranque no se realizará correctamente. Si debe realizar cambios en la partición de un disco encriptado, desencripte el disco primero y luego realice los cambios.
- **Utilización de CHKDSK**: CHKDSK puede informar errores en un archivo llamado PGPWDE01 cuando verifica un disco que se ha encriptado con PGP Whole Disk Encryption. Estos errores pueden ignorarse porque este archivo está protegido con PGP Whole Disk Encryption. [20197]
- **Utilización de uso de CPU máximo para encriptar los discos extraíbles**: los discos extraíbles no pueden encriptarse con la opción Uso de CPU máximo, si bien esta opción pueda seleccionarse. [24286]
- **PGP WDE en sistemas Lenovo Ideapad**: PGP WDE no es compatible con los sistemas Lenovo Ideapad S10-2 que se ejecutan en Microsoft Windows XP. PGP WDE es compatible si se ejecuta en Windows 7 en estos sistemas. [24082]
- **Encriptación automática de la partición de arranque**: Si la política de PGP Universal Server requiere una encriptación automática sólo de la partición de arranque, y ésta se encuentra en el disco 1 (no el disco 0), se

encriptará todo el disco (ambas particiones). [25127]

- **Actualizaciones del sistema operativo durante la encriptación**: Mientras se esté encriptando el disco, no acepte ninguna actualización del sistema operativo que pueda aparecer. Si la actualización se realiza automáticamente, no reinicie la computadora hasta que el proceso de encriptación haya finalizado. [25451, 25612]
- **Compatibilidad con computadoras portátiles Sony VAIO**: PGP WDE es compatible con Windows XP que sólo se ejecuta en computadoras portátiles Sony VAIO Sony BIOS versión T4350M3. Otras versiones de BIOS no son compatibles. Éste es un problema reconocido por Sony. [23556]
- **Ingreso de caracteres de dos bytes del alfabeto japonés para la recuperación de la frase de contraseña**: Cuando haya olvidado la frase de contraseña y haya respondido las preguntas para habilitar la recuperación de la frase de contraseña, podrá ingresar los caracteres de dos bytes del alfabeto japonés. Para hacerlo, seleccione **Olvidé mi frase de contraseña** en PGP BootGuard. Para comenzar, el primer carácter debe ingresarse como un carácter en mayúscula. Ingrese el carácter en mayúscula y presione Enter (para aceptar el carácter) o presione la barra de espacio dos veces para seleccionar el carácter en minúscula. (Al crear las preguntas en PGP Desktop, asegúrese de haber activado los caracteres de dos bytes en IME japonés.) [26228]

PGP Zip

- **PGP Zip y PGP NetShare**: En Windows Vista, no se puede crear un archivo de PGP Zip de una carpeta agregada a PGP NetShare. [17058]
- **Archivo de desencriptado automático:** cuando el destinatario desencripta un archivo de desencriptado automático (SDA), todos los cuadros de diálogo que muestra PGP Desktop están en inglés, independientemente de la versión de PGP Desktop (inglés, alemán o japonés) que se utilizó para crear el SDA e independientemente del idioma que tiene su sistema actualmente. Esto se aplica a todos los cuadros de diálogo que aparecen. Los nombres de los archivos y el contenido del SDA no se ven afectados. [7144]
- **Compatibilidad con AVG Anti-Virus**: para crear un PGP Zip SDA en sistemas con el software AVG Anti-Virus, debe utilizar la versión 8.0 o superior de AVG Anti-Virus. Si está utilizando una versión anterior, deshabilite el análisis heurístico en RESIDENT SHIELD si desea crear los PGP Zip SDA. [16488]

Cómo obtener ayuda

Información de contacto

Cómo comunicarse con el soporte técnico

- Para obtener información sobre las opciones de soporte técnico para PGP y cómo comunicarse con éste, visite la página de inicio de soporte técnico de PGP Corporation.
- Para tener acceso a la base de conocimientos de soporte técnico para PGP o solicitar soporte técnico de PGP, visite el sitio web del portal de soporte técnico para PGP. **Tenga en cuenta que es posible que tenga acceso a partes de la Base de conocimientos de soporte técnico para PGP sin un acuerdo de soporte técnico; sin embargo, debe tener un acuerdo de soporte técnico válido para solicitarlo.**
- Para tener acceso a los foros de soporte técnico para PGP, visite Soporte técnico para PGP. En PGP Corporation, puede encontrar alojados foros de soporte técnico de la comunidad de usuarios.

Cómo comunicarse con servicio de atención al cliente

- Para obtener ayuda con pedidos, descargas y licencias, visite Servicio de atención al cliente de PGP Corporation.

Cómo comunicarse con otros departamentos

- En caso de necesitar otro tipo de contacto con PGP Corporation, visite la página de contactos de PGP.
- Para obtener información general sobre PGP Corporation, visite el sitio web de PGP.

Documentación disponible

Antes de la instalación, la documentación completa del producto está disponible en el Portal de soporte técnico para

PGP Corporation.

A menos que se indique lo contrario, la ayuda en pantalla está disponible con el producto PGP Desktop. Las notas de la versión, que pueden contener información actualizada de último momento que no se encuentre en la documentación del producto, también están disponibles. La guía del usuario y la guía de inicio rápido, que se proporcionan en formato PDF, están disponibles en el Portal de soporte técnico para PGP Corporation.

Una vez que PGP Desktop se lanza al mercado, se ingresa información adicional sobre el producto en la base de conocimientos en línea disponible en la Base de conocimientos de soporte técnico para PGP.

Derechos de autor y marcas comerciales

Copyright © 1991-2010 PGP Corporation. Todos los derechos reservados. "PGP", "Pretty Good Privacy" y el logotipo de PGP son marcas comerciales registradas, y PGP Universal es una marca comercial de PGP Corporation en los Estados Unidos y otros países. Las demás marcas comerciales registradas y no registradas en este documento son propiedad de sus respectivos dueños.